ESET MOBILE SECURITY

FÜR ANDROID

Benutzerhandbuch

(für Produktversion 2.0 und höher)

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen

ESET **MOBILE SECURITY**

© ESET, spol. s r.o.
ESET Mobile Security wurde entwickelt von ESET, spol. s r.o.
Weitere Informationen finden Sie unter www.eset.com.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung an jedem der hier beschriebenen Software-Produkte Änderungen vorzunehmen.

Support: www.eset.com/support

Stand 23. 8. 2013

Inhalt

1. Einführung 3
1.1 Neuerungen 3
1.2 Systemanforderungen 3
2. Installation 4
2.1 Installation über die ESET-Website 4
2.2 Installation über Google Play 4
2.3 Installation über Amazon 4
2.4 Startassistent 4
2.5 Deinstallation 5
3. Lizenz 6
4. Virenschutz 7
4.1 Quarantäne 8
4.2 Scan-Logs 8
4.3 Erweiterte Einstellungen 8
5. Anti-Theft 10
5.1 SIM-Schutz 10
5.1.1 Hinzufügen einer neuen vertrauenswürdigen SIM 10
5.2 Meine Kontaktdetails 10
5.3 Vertrauenswürdige Freunde 10
5.3.1 Hinzufügen eines neuen vertrauenswürdigen Freunds 11
5.4 SMS-Textbefehle 11
6. SMS- und Anruffilter 12
6.1 Regeln 12
6.1.1 Hinzufügen einer neuen Regel 12
6.2 Verlauf 13
7. Phishing-Schutz 14
8. Sicherheits-Audit 15
8.1 Geräteüberwachung 15
8.2 Anwendungsaudit 15
9. Einstellungen 16
9.1 Sicherheitspasswort 16
10. Support 17

1. Einführung

ESET Mobile Security ist eine umfassende Sicherheitslösung, die Ihr Gerät vor Bedrohungen und Phishing-Seiten schützt, unerwünschte Anrufe und Nachrichten filtert und Ihnen ermöglicht, Ihr Gerät bei Verlust oder Diebstahl remote zu steuern.

1.1 Neuerungen

Im Vergleich zu Version 1.2 enthält ESET Mobile Security 2 folgende Neuerungen und Verbesserungen:

Tablet-Unterstützung
Das neue Design eignet sich für die Nutzung auf Tablets im Hoch- und Querformat. Auf Geräten, die keine Anruf- und Nachrichtenfunktion unterstützen, werden bestimmte Funktionen (z. B. Anti-Theft) nicht angezeigt.

Phishing-Schutz
Schützen Sie sich vor schädlichen Websites, die versuchen, sich Ihre vertraulichen Informationen wie Benutzernamen, Passwörter, Bankdaten oder Kreditkartendetails anzueignen.

Geplante Prüfung
Legen Sie regelmäßige Malware-Prüfungen auf einen Wunschzeitpunkt, zum Beispiel nachts.

Zeitgesteuerter SMS- und Anruffilter
Blockieren Sie Anrufe und SMS nur zu bestimmten Zeiten und lassen Sie Ausnahmen für Familienmitglieder und Freunde zu. Anhand der Android-Kontaktgruppen (Familie, Freunde, Arbeit) können Sie Regeln für jede Gruppe definieren.

ESET Live Grid
Unsere Cloud-Technologie sammelt Malware-Proben von ESET-Produktbenutzern weltweit und bietet dadurch schnellen Schutz vor den neuesten Bedrohungen.

Fern-Alarm
Sie können Ihr Gerät durch Aktivierung eines Sirenentons auffinden, selbst wenn es stummgeschaltet ist.

Erkennung eventuell unerwünschter Anwendungen
Hiermit werden Apps erkannt, die Schäden durch unbefugten Zugriff auf Gerätedaten oder -funktionen verursachen können. Die Früherkennung schützt Sie vor dem unbefugten Versand von SMS und vor Anrufen bei teuren Premiumdiensten.

Geräteüberwachung
Diese Funktion liefert Informationen zum Status von Daten- und Telefonie-Roaming, zur aktuellen WLAN-Verbindung und zum verfügbaren Speicher.

Anwendungsaudit
Hiermit sehen Sie die Berechtigungen aller installierten Apps, übersichtlich in Gruppen geordnet. So sehen Sie sofort, welche App auf welche Gerätedaten zugreifen kann.

Neues Design
Die grafische Benutzeroberfläche, das Hauptprogrammfenster und die die Programmeinstellungen wurden komplett überarbeitet und sind nun intuitiv und einfacher zu bedienen.

1.2 Systemanforderungen

Für die Installation von ESET Mobile Security muss Ihr Android-Gerät folgende Mindestsystemanforderungen erfüllen:

Betriebssystem: Android 2.3 (Gingerbread) oder höher
Touchscreen-Auflösung: mindestens 240 x 320 px, 320 x 480 px empfohlen
CPU: 500 MHz
RAM: 256 MB
Verfügbarer interner Speicherplatz: 12 MB

HINWEIS: Gerootete Geräte werden nicht unterstützt. Bestimmte Funktionen (z. B. Anti-Theft und SMS- und Anruffilter) sind auf Tablets, die keine Anruf- und Nachrichtenfunktion unterstützen, nicht verfügbar.

2. Installation

Zur Installation von ESET Mobile Security stehen Ihnen die folgenden Methoden zur Verfügung:

HINWEIS: Wenn Sie bereits einen aktiven Benutzernamen mit Passwort oder einen Aktivierungscode von ESET erhalten haben, laden Sie ESET Mobile Security bitte von der ESET Website herunter.

2.1 Installation über die ESET-Website

Laden Sie ESET Mobile Security herunter, indem Sie den folgenden QR-Code mit Ihrem Mobilgerät und einer App wie QR Droid oder Barcode Scanner einscannen.

Alternativ können Sie die APK-Installationsdatei für ESET Mobile Security auf Ihrem Computer herunterladen:

1. Laden Sie die Datei von der ESET-Website herunter.
2. Kopieren Sie die Datei per Bluetooth oder über den USB-Anschluss auf Ihr Gerät.
3. Tippen Sie auf dem Android-Hauptbildschirm auf das Übersichtssymbol oder auf **Startseite** > **Menü**, und tippen Sie auf **Einstellungen** > **Anwendungen**. Achten Sie darauf, dass die Option **Unbekannte Herkunft** aktiviert ist.
4. Suchen Sie die APK-Datei mit einem Dateimanager wie ASTRO File Manager oder ES File Explorer.
5. Öffnen Sie die Datei und tippen Sie auf **Installieren**. Nachdem die App installiert wurde, tippen Sie auf **Öffnen**.

2.2 Installation über Google Play

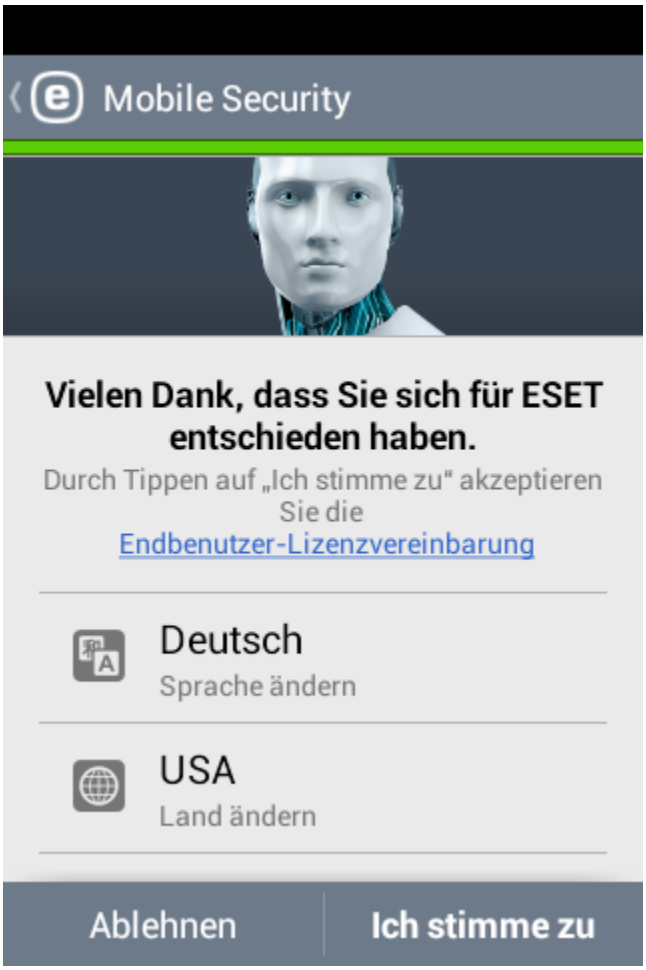
Öffnen Sie die Google Play Store-App auf Ihrem Android-Gerät und suchen Sie nach ESET Mobile Security (oder einfach nach Eset).

Alternativ können Sie das Programm installieren, indem Sie den folgenden QR-Code mit Ihrem Mobilgerät und einer App wie QR Droid oder Barcode Scanner einscannen:

2.3 Installation über Amazon

Öffnen Sie die Amazon-App auf Ihrem Android-Gerät und suchen Sie nach ESET Mobile Security (oder einfach nach Eset).

2.4 Startassistent

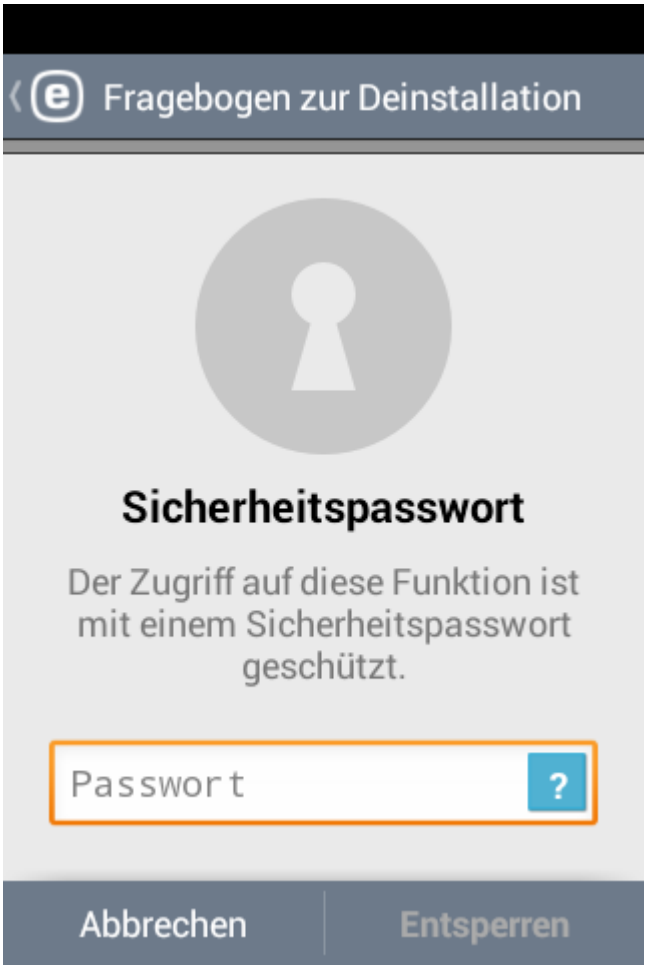


Befolgen Sie nach der Installation der App auf Ihrem Gerät die Anweisungen im Startassistenten:

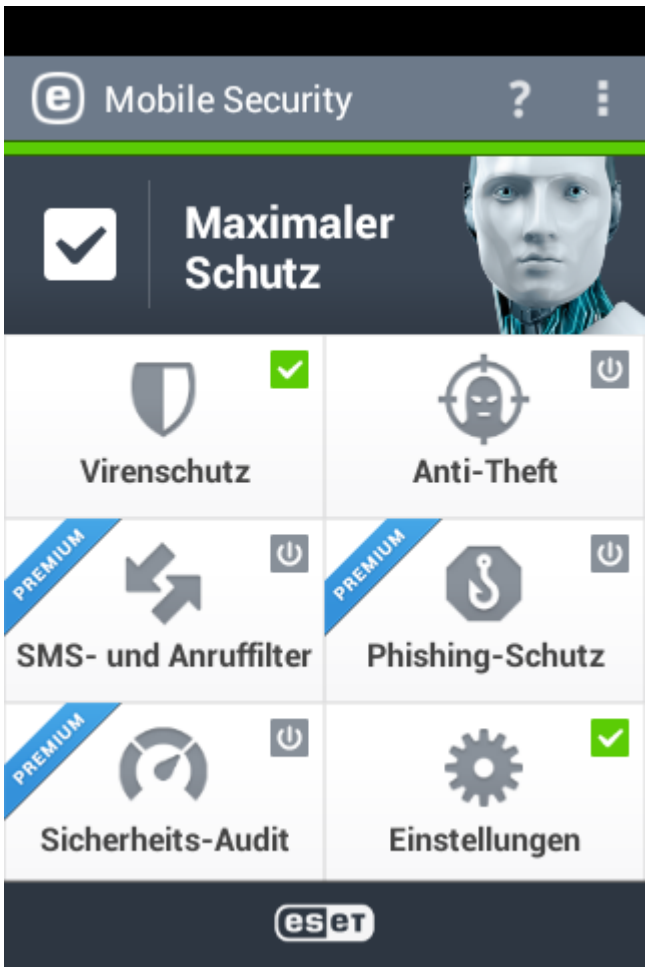
1. Wählen Sie die Sprache aus, die Sie in ESET Mobile Security verwenden möchten.
2. Wählen Sie das Land aus, in dem Sie wohnen.
3. Wenn Sie durch das Senden anonymer Daten über die Anwendungsnutzung zur Weiterentwicklung der ESET-Produkte beitragen möchten, aktivieren Sie die entsprechende Option.
4. Tippen Sie auf **Ich stimme zu**. Dadurch akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.
5. Wählen Sie im nächsten Schritt, ob Sie an ESET Live Grid teilnehmen möchten. Weitere Informationen zu ESET Live Grid finden Sie in diesem Abschnitt 8.
6. Tippen Sie auf **Weiter**.
7. Geben Sie an, ob ESET Mobile Security auch eventuell unerwünschte Anwendungen erkennen soll. Weitere Informationen zu dieser Art von Anwendungen finden Sie in diesem Abschnitt 8.
8. Tippen Sie auf **Weiter**.
9. Tippen Sie auf **Fertig stellen**.

2.5 Deinstallation

Wenn Sie ESET Mobile Security deinstallieren möchten, verwenden Sie den Deinstallationsassistenten unter **Einstellungen** > **Deinstallieren** im Hauptmenü von ESET Mobile Security. Wenn Sie zuvor den Deinstallationsschutz aktiviert hatten, werden Sie um Eingabe Ihres Sicherheitspassworts gebeten.



3. Lizenz



Nach erfolgreicher Installation muss ESET Mobile Security aktiviert werden. Um den Bereich **Lizenz** zu öffnen, tippen Sie auf das Menüsymbol im Hauptbildschirm von ESET Mobile Security (oder drücken Sie die Taste **MENÜ** am Gerät) und tippen Sie auf **Lizenz**.

Die Aktivierungsmethode hängt davon ab, ob Sie ESET Mobile Security von der ESET-Website, über Amazon oder über Google Play heruntergeladen haben.

- **Kostenlose Probeversion** – Wählen Sie diese Option, wenn Sie keine Lizenz besitzen und ESET Mobile Security vor dem Kauf testen möchten. Geben Sie Ihre **E-Mail-Adresse** ein, um ESET Mobile Security für einen begrenzten Zeitraum zu aktivieren. Nach der erfolgreichen Produktaktivierung erhalten Sie eine E-Mail mit einer Bestätigung. Eine Probelizenz kann nur einmal pro Gerät aktiviert werden.
- **Aktivierung mit Benutzername und Passwort** - Wenn Sie das Produkt von einem ESET-Vertriebshändler erworben haben, haben Sie beim Kauf einen Benutzernamen und ein Passwort erhalten. Geben Sie diese Daten in den Feldern **Benutzername** und **Passwort** ein.
- **Aktivierung mit Aktivierungscode** - Wenn Sie das Programm mit einem neuen Gerät oder in einer Verkaufspackung erworben haben, haben Sie beim Kauf einen Aktivierungscode erhalten. Geben Sie diesen Code im Feld **Aktivierungscode** und Ihre aktuelle E-Mail-Adresse im Feld **E-Mail-Adresse** ein. Ihre neuen Authentifizierungsdaten (Benutzer und Passwort) ersetzen automatisch den Aktivierungscode. Sie werden Ihnen an die angegebene E-Mail-Adresse zugesendet.
- **Lizenz kaufen** - Wählen Sie diese Option, wenn Sie noch keine Lizenz haben und eine erwerben möchten. Sie werden zur Website Ihres örtlichen ESET-Vertriebshändlers weitergeleitet.

Jede Lizenz ist nur für einen begrenzten Zeitraum gültig. Nach dem Ablauf der Lizenz werden Sie zur Verlängerung aufgefordert (Sie erhalten vor dem Ablauf im Programm einen Hinweis).

HINWEIS: Während der Aktivierung muss das Gerät mit dem Internet verbunden sein. Es wird eine kleine Datenmenge heruntergeladen.

4. Virenschutz

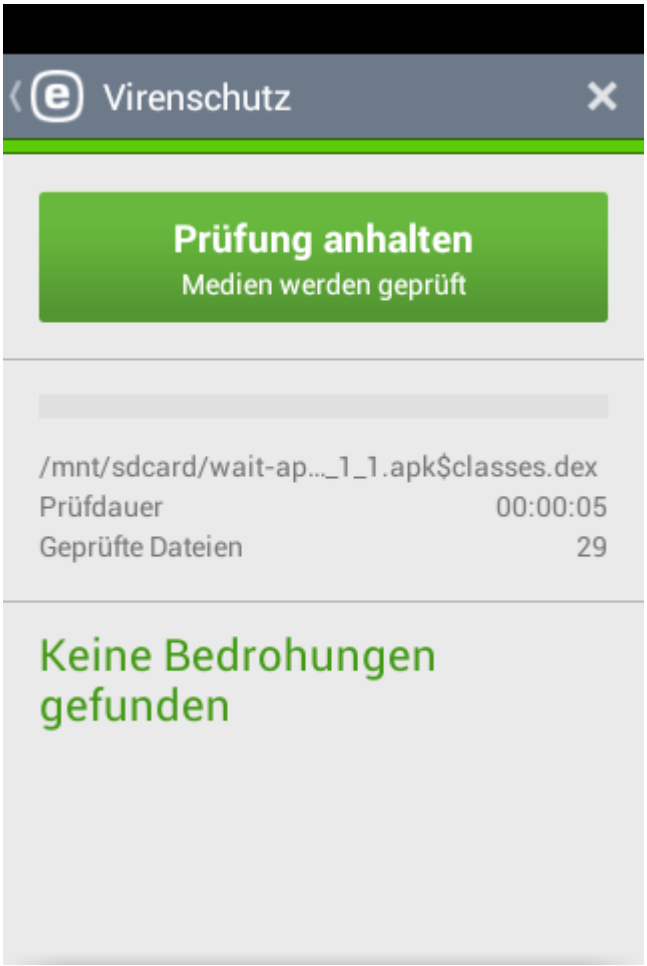
Das Virenschutzmodul schützt Ihr Gerät vor Schadcode, indem es Bedrohungen abwehrt und sie dann entfernt oder in die Quarantäne verschiebt.

Gerät prüfen

Mit der Option **Gerät prüfen** können Sie Ihr Mobilgerät auf Infiltrationen (eingedrungene Schadsoftware) überprüfen.

Bestimmte vordefinierte Dateitypen werden standardmäßig geprüft. Bei einer Prüfung des gesamten Geräts werden der Arbeitsspeicher, ausgeführte Prozesse, die dazugehörigen Funktionsbibliotheken und Dateien geprüft, die sich im internen Speicher oder auf Wechselmedien befinden. Eine Zusammenfassung der Prüfung wird in einer Log-Datei gespeichert, auf die Sie über den Abschnitt **Logs** zugreifen können.

Wenn Sie eine aktuell ausgeführte Prüfung abbrechen möchten, tippen Sie auf das Symbol .



Prüfstufe

Sie können aus 3 verfügbaren Prüfstufen auswählen:

- **Schnell**: Wenn Sie diese Option auswählen, prüft ESET Mobile Security nur installierte Anwendungen, DEX-Dateien (ausführbare Dateien für das Android-Betriebssystem), SO-Dateien (Bibliotheken) und ZIP-Dateien mit maximal 3 verschachtelten Archiven.
- **Smart**: Die Smart-Prüfung prüft zusätzlich zu den von der Schnellprüfung geprüften Elementen den Inhalt von SD-Karten.
- **Tief**: Alle Dateitypen werden unabhängig von ihrer Erweiterung im internen Speicher und auf der SD-Karte geprüft.

Geplante Prüfung

Mit der Option **Geplante Prüfung** können Sie eine regelmäßige automatische Geräteprüfung zu vordefinierten Zeiten einrichten. Um eine Prüfung zu planen, tippen Sie auf die Schaltfläche neben der Option **Geplante Prüfung** und legen Sie das Datum und die Uhrzeit für den Beginn der Prüfung fest. Standardmäßig sind alle Wochentage ausgewählt.

Quarantäne

Hauptzweck der Quarantäne ist die sichere Verwahrung infizierter Dateien. Weitere Informationen finden Sie im Abschnitt Quarantäne 8.

Scan-Logs

Der Bereich **Scan-Logs** enthält Logs mit umfassenden Daten zu abgeschlossenen Scans. Weitere Informationen finden Sie in diesem Kapitel 8.

Bedrohungsdatenbank aktualisieren

In ESET Mobile Security sind automatische Updates standardmäßig aktiviert, damit das Programm regelmäßig aktualisiert wird. Um manuell ein Update zu starten, tippen Sie auf **Bedrohungsdatenbank aktualisieren**.

HINWEIS: Updates werden nur bei Bedarf ausgegeben, also wenn eine neue Bedrohung hinzugefügt wurde. So wird vermieden, dass unnötig Bandbreite in Anspruch genommen wird. Die Updates sind im Rahmen Ihrer aktiven Lizenz kostenlos. Für die Datenübertragung können jedoch bei Ihrem Mobilfunkanbieter Gebühren anfallen.

Eine detaillierte Beschreibung der **Erweiterten Einstellungen** für den Virenschutz finden Sie im Bereich Erweiterte Einstellungen 8.

4.1 Quarantäne

Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Mobile Security fälschlicherweise erkannt worden sind.

Die Dateien in der Quarantäne können in einem Log angezeigt werden, das Datum und Uhrzeit der Quarantäne und den Namen und ursprünglichen Speicherort der infizierten Dateien enthält.

Um eine Datei aus der Quarantäne an ihrem ursprünglichen Speicherort wiederherzustellen, tippen Sie auf die Datei und dann auf das Symbol . Es wird nicht empfohlen, die Dateien aus der Quarantäne regelmäßig wiederherzustellen.

Um eine Datei aus der Quarantäne dauerhaft von Ihrem Gerät zu entfernen, tippen Sie auf die Datei und dann auf das Symbol .

HINWEIS: Wenn eine verdächtige Anwendung in die Quarantäne verschoben wird, Sie die Anwendung jedoch später installieren, wird die Anwendung automatisch aus der Quarantäne entfernt.

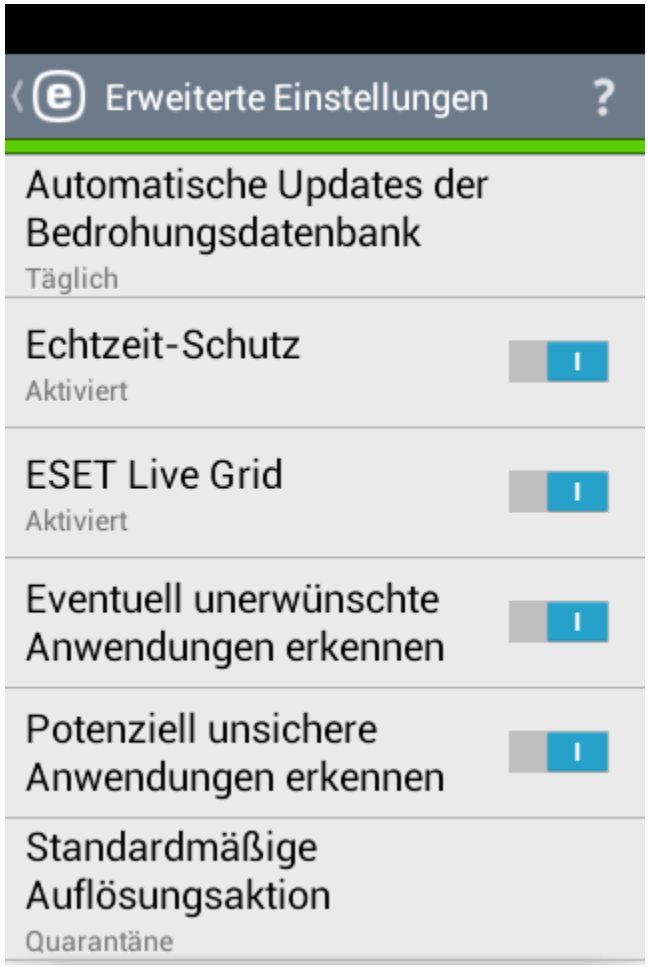
4.2 Scan-Logs

Scan-Logs werden nach jeder geplanten Prüfung und jeder manuell ausgelösten Geräteprüfung erstellt.

Jeder Log-Eintrag enthält die folgenden Angaben:

- Datum und Uhrzeit des Ereignisses
- Dauer der Prüfung
- Anzahl der geprüften Dateien
- Prüfergebnis oder während der Prüfung aufgetretene Fehler

4.3 Erweiterte Einstellungen



Automatische Updates der Bedrohungsdatenbank
Mit dieser Option können Sie festlegen, in welchen Zeitabständen Bedrohungsdatenbank-Updates automatisch heruntergeladen werden. Die Updates werden je nach Bedarf beim Hinzufügen einer neuen Bedrohung zur Datenbank herausgegeben. Wir empfehlen, für diese Einstellung den Standardwert (täglich) beizubehalten.

Echtzeit-Schutz
Mit dieser Option können Sie den Echtzeit-Scanner aktivieren/deaktivieren. Der Scanner wird automatisch beim Starten des Systems gestartet und prüft Dateien, die Sie verwenden. Der Scanner prüft automatisch den Ordner *Downloads* alle *.apk*-Installationsdateien und alle Dateien auf eingeführten SD-Karten.

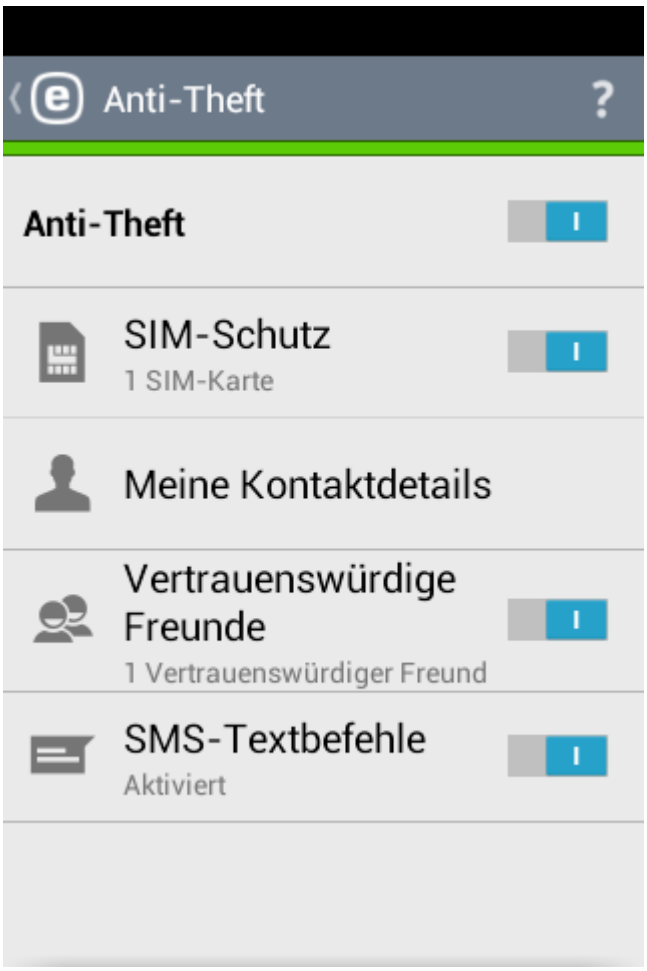
ESET Live Grid
ESET Live Grid basiert auf dem ThreatSense.Net-Frühwarnsystem und bietet zusätzlichen Schutz für Ihr Gerät. Es überwacht die im System ausgeführten Programme und Prozesse und nutzt dabei die neuesten Informationen, die von Millionen von ESET-Benutzern weltweit zur Verfügung gestellt werden. Die ESET Live Grid-Datenbank wird ständig aktualisiert und erweitert und ermöglicht so immer schnellere und genauere Prüfungen. Sie gewährleistet einen besseren proaktiven Schutz und eine höhere Prüfgeschwindigkeit, von der alle unsere Benutzer profitieren. Wir empfehlen, diese Funktion zu aktivieren. Vielen Dank für Ihre Unterstützung.

Eventuell unerwünschte Anwendungen erkennen
Eine unerwünschte Anwendung ist ein Programm, das Adware enthält, Symbolleisten installiert, Suchergebnisse verfolgt oder andere nicht genau bekannte Ziele verfolgt. In bestimmten Fällen möchten Sie jedoch möglicherweise die Risiken einer solchen Software in Kauf nehmen, um ihre Funktionen zu nutzen. Daher weist ESET dieser Art Anwendung eine niedrigere Risikokategorie zu als anderen Arten von Schadsoftware.

Potenziell unsichere Anwendungen erkennen
Es gibt eine Vielzahl legitimer Anwendungen, deren Funktionen die Administration von Netzwerkgeräten erleichtern. Diese Anwendungen können jedoch auch zu schädlichen Zwecken missbraucht werden. Mit der Option **Potenziell unsichere Anwendungen erkennen** können Sie derartige Bedrohungen aufdecken. Die Klassifizierung „potenziell unsichere Anwendungen“ wird für kommerzielle, legitime Software verwendet. Dies betrifft beispielsweise Remotezugriff-Anwendungen, Anwendungen zur Passwortentschlüsselung und Keylogger.

Standardmäßige Aktion
Diese Einstellung legt fest, welche Aktion ausgeführt wird, wenn bei einer Prüfung Bedrohungen erkannt wurden. Mit **Entfernen** wird die infizierte Datei gelöscht. Mit der Option **Quarantäne** wird die infizierte Datei in die Quarantäne 8 verschoben.

5. Anti-Theft



Die Anti-Theft-Funktion schützt Ihr Mobilgerät vor unerlaubtem Zugriff.

Wenn Sie Ihr Gerät verlieren oder es gestohlen wird und jemand eine neue (nicht vertrauenswürdige) SIM-Karte in das Gerät einlegt, sperrt ESET Mobile Security automatisch das Gerät und sendet eine SMS-Warnmeldung an die vom Benutzer definierten Telefonnummern. Diese Nachricht enthält die Telefonnummer der aktuell verwendeten SIM-Karte, die IMSI-Nummer (International Mobile Subscriber Identity) und die IMEI-Nummer des Telefons (International Mobile Equipment Identity). Dem nicht autorisierten Benutzer ist nicht bewusst, dass diese Nachricht gesendet wurde, da sie automatisch aus dem Nachrichtenordner entfernt wird. Außerdem können Sie ein verloren gegangenes Mobilgerät über seine GPS-Koordinaten orten lassen oder alle darauf gespeicherten Daten aus der Ferne löschen.

HINWEIS: Die Anti-Theft-Funktion funktioniert nicht auf Tablets, die keine Textnachrichten unterstützen.

Tippen Sie im Hauptprogrammmenü auf **Anti-Theft**, um den Anti-Theft-Schutz zu aktivieren. Ein Assistent führt Sie durch einige einfache Schritte: Aktivieren des Deinstallationsschutzes, Hinzufügen von ESET Mobile Security als Geräteadministrator, Erstellen Ihres Sicherheitspassworts und Erstellen eines Passworts für SMS-Textbefehle.

Ihr **Sicherheitspasswort** wird zum Entsperren des Geräts, zum Zugriff auf passwortgeschützte Funktionen (z. B. Anti-Theft) und zur Deinstallation von ESET Mobile Security benötigt. Ihr **Passwort für SMS-Textbefehle** wird zum Senden von Textbefehlen verwendet. Weitere Informationen zu Textbefehlen finden Sie in diesem Abschnitt 11.

WICHTIGER HINWEIS: Wählen Sie Passwörter sorgsam aus. Kombinieren Sie Klein- und Großbuchstaben und Zahlen, um die Passwortstärke zu erhöhen und anderen Personen das Erraten Ihres Passworts zu erschweren.

5.1 SIM-Schutz

Der Bereich **SIM-Schutz** enthält die Liste der vertrauenswürdigen SIM-Karten, die von ESET Mobile Security akzeptiert werden. Wenn eine nicht in der Liste definierte SIM-Karte eingelegt wird, wird der Bildschirm gesperrt und Ihren **Vertrauenswürdigen Freunden** wird eine Warnmeldungs-SMS gesendet.

Um eine neue SIM-Karte hinzuzufügen, tippen Sie auf das Symbol ✚. Weitere Informationen finden Sie in diesem Abschnitt 10.

Um eine SIM-Karte aus der Liste zu entfernen, tippen Sie auf den Eintrag und halten Sie ihn ausgewählt. Tippen Sie dann auf das Symbol 🗑.

5.1.1 Hinzufügen einer neuen vertrauenswürdigen SIM

Füllen Sie das Feld **Name der SIM-Karte** aus (z. B. „privat“, „geschäftlich“) und geben Sie die **IMSI** (International Mobile Subscriber Identity)-Nummer ein. Die IMSI-Nummer ist üblicherweise eine 15-stellige Zahl, die auf der SIM-Karte aufgedruckt ist. In bestimmten Fällen kann die IMSI-Nummer auch kürzer sein.

5.2 Meine Kontaktdetails

Im Feld **Meine Kontaktdetails** können Sie den Text festlegen, der an die vorab festgelegte(n) Nummer(n) gesendet wird, nachdem eine nicht vertrauenswürdige SIM in Ihr Gerät eingesetzt wurde. Geben Sie eine Gerätebeschreibung und eine alternative Kontaktnummer (z. B. private oder geschäftliche Festnetznummer) oder eine E-Mail-Adresse ein.

5.3 Vertrauenswürdige Freunde

In der Liste **Vertrauenswürdige Freunde** können Sie mit Telefonnummern definieren, die eine Alarm-SMS erhalten sollen, wenn eine nicht vertrauenswürdige SIM-Karte in Ihr Gerät eingesetzt wurde. Um einen neuen vertrauenswürdigen Freund hinzuzufügen, tippen Sie auf **Aus Kontakten hinzufügen** und wählen Sie einen Kontakt aus der Kontaktliste aus.

Wenn die gewünschte Person nicht in der Kontaktliste

enthalten ist, tippen Sie auf das Symbol ✚. Weitere Informationen finden Sie in diesem Abschnitt 11.

Um einen Kontakt aus der Liste zu entfernen, tippen Sie auf den Kontakt und halten Sie ihn ausgewählt. Tippen Sie dann auf das Symbol 🗑.

HINWEIS: Wenn Sie im Ausland unterwegs sind, müssen Sie den Rufnummern in der Liste die Landesvorwahl hinzufügen (z. B. +49 711 123).

5.3.1 Hinzufügen eines neuen vertrauenswürdigen Freunds

Geben Sie den Namen des Freunds und die entsprechende Telefonnummer ein. Wenn der Kontakt mehrere Telefonnummern enthält, wird die Alarm-SMS an alle diese Telefonnummern gesendet. Wenn Sie zulassen möchten, dass dieser Freund Ihr Passwort zurücksetzen kann, falls Sie es vergessen, wählen Sie die Option **Remote-Zurücksetzen des Passworts zulassen** aus.

5.4 SMS-Textbefehle

SMS-Remotebefehle (lock, siren, find, wipe) funktionieren nur, wenn die Option **SMS-Textbefehle** aktiviert ist.

Wenn Sie Ihr Gerät verloren haben und es sperren möchten, senden Sie von einem beliebigen Mobilgerät eine SMS im folgenden Format an Ihre Telefonnummer:
eset lock Passwort
Ersetzen Sie *Passwort* mit Ihrem Sicherheitspasswort. Nachdem Ihr Gerät gesperrt wurde, kann es nur von einem autorisierten Benutzer durch die Eingabe Ihres Passworts entsperrt werden.

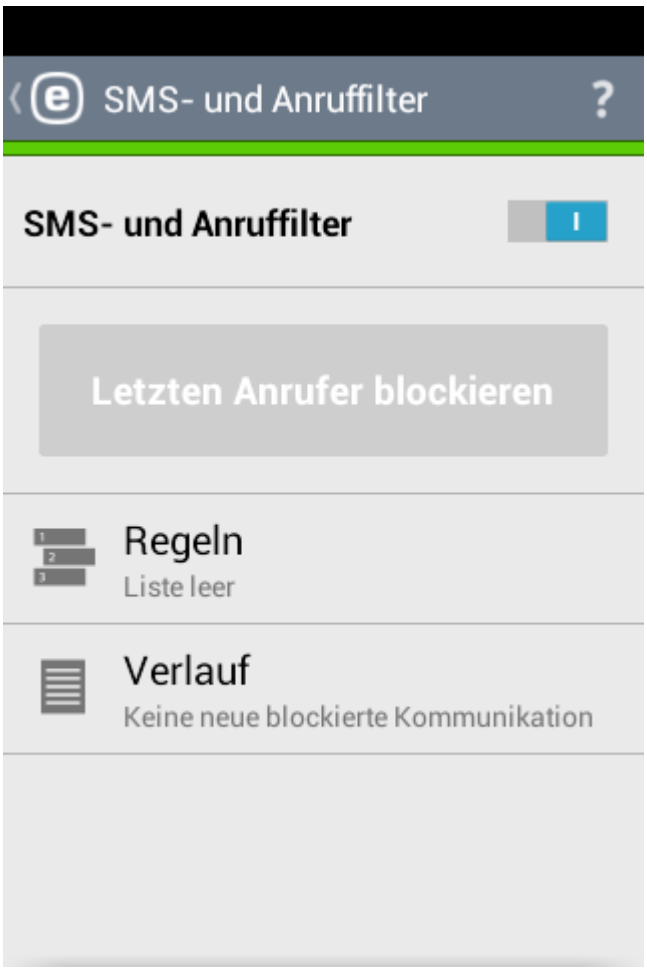
Um das Gerät zu sperren und einen Signalton wiederzugeben, senden Sie eine SMS mit folgendem Befehl an Ihre Mobiltelefonnummer:
eset siren Passwort

Um die GPS-Koordinaten Ihres Mobilgeräts abzufragen, senden Sie eine SMS mit dem folgenden Format an Ihre Mobilfunknummer bzw. die Nummer der aktuell eingelegten SIM-Karte (falls die SIM-Karte bereits ersetzt wurde):
eset find Passwort
Sie erhalten eine SMS mit Angaben zum ungefähren Standort des verlorenen Geräts und eine weitere SMS mit den genauen GPS-Koordinaten des Geräts, die außerdem eine Verknüpfung zu diesem Standort bei Google Maps enthält. Beachten Sie, dass die GPS-Koordinaten nur gesendet werden können, wenn das GPS-Modul Ihres Mobilgeräts zuvor bereits aktiviert wurde.

Um alle auf dem Gerät und ggf. eingelegten Wechselmedien gespeicherten Daten zu löschen, senden Sie eine SMS im folgenden Format an das Mobilgerät:
eset wipe Passwort
Alle Kontakte, Nachrichten, E-Mails und installierten Apps, Ihr Google-Konto sowie der Inhalt der SD-Karte werden dann endgültig vom Gerät gelöscht. Wenn ESET Mobile Security nicht als Geräteadministrator eingerichtet ist, werden nur Kontakte, Nachrichten und der Inhalt der SD-Karte gelöscht.

HINWEIS: Beim Passwort muss die Groß- und Kleinschreibung berücksichtigt werden. Geben Sie das Passwort also genau so ein, wie Sie es im Anti-Theft-Einrichtungsassistenten definiert haben.

6. SMS- und Anruffilter



Der **SMS- und Anruffilter** blockiert auf Grundlage der von Ihnen definierten Regeln eingehende SMS/MMS und ein- und ausgehende Anrufe.

Solche unerwünschten Nachrichten sind zum Beispiel Werbung von Mobilfunkanbietern oder Nachrichten von unbekannten Benutzern. Der Ausdruck *Nachricht blockieren* bezieht sich auf das automatische Verschieben von eingehenden Nachrichten in den Bereich **Verlauf**. Es wird kein Hinweis angezeigt, wenn eine eingehende Nachricht blockiert wird. Der Vorteil dieses Verfahrens besteht darin, dass Sie einerseits nicht durch unerwünschte Informationen belästigt werden, andererseits jedoch auch die Logs nach Nachrichten durchsuchen können, die fälschlicherweise blockiert worden sind.

HINWEIS: Der SMS- und Anruffilter funktioniert nicht auf Tablets, die keine Anruf- und Nachrichtenfunktion unterstützen.

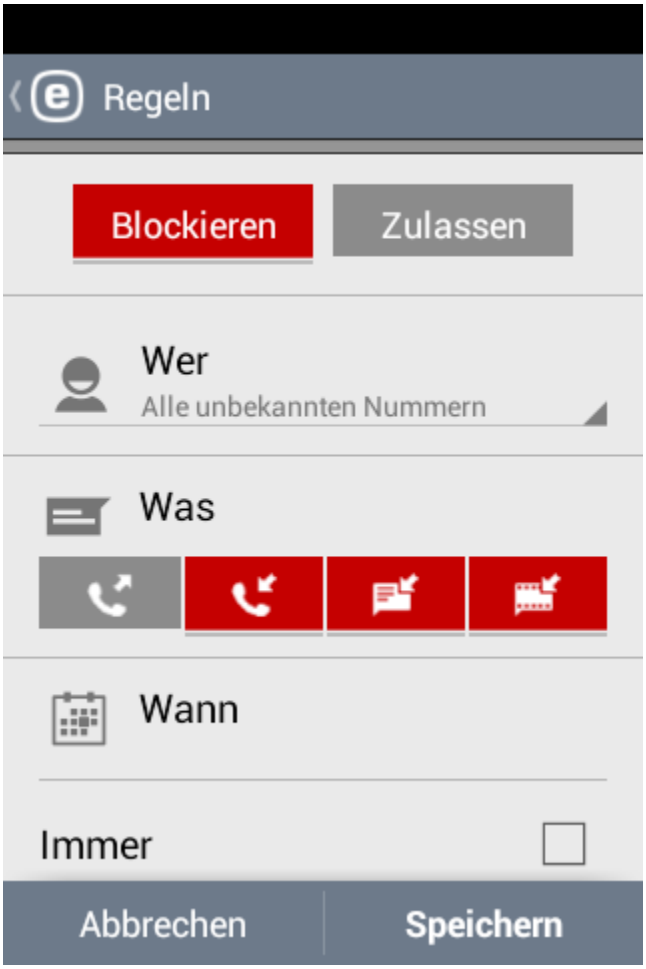
Um Anrufe und Nachrichten von der zuletzt eingegangenen Telefonnumer zu blockieren, tippen Sie **Letzten Anrufer blockieren**. Dadurch wird eine neue Regel für den SMS- und Anruffilter erstellt.

6.1 Regeln

Um eine neue Regel hinzuzufügen, tippen Sie auf das Symbol ➕. Weitere Informationen zum Erstellen neuer Regeln finden Sie in diesem Abschnitt 12.

Um einen bestehenden Regeleintrag aus der Liste **Regeln** zu entfernen, berühren Sie den Eintrag und halten Sie ihn ausgewählt. Tippen Sie dann auf das Symbol 🗑.

6.1.1 Hinzufügen einer neuen Regel



Geben Sie eine Telefonnummerngruppe oder eine Person an. **Alle unbekannten Nummern** umfasst alle Telefonnummern, die nicht in der Kontaktliste gespeichert sind. Diese Option können Sie verwenden, um unerwünschte Telefonanrufe (z. B. von Telemarketing-Firmen) zu unterbinden oder um zu verhindern, dass Kinder unbekannte Nummern wählen. **Alle bekannten Nummern** umfasst alle in der Kontaktliste gespeicherten Telefonnummern. **Unterdrückte Nummern** gilt für Anrufer, die über die Rufnummernunterdrückung bewusst festlegen, dass ihre Rufnummer nicht angezeigt wird.

Legen Sie fest, was blockiert bzw. zugelassen werden soll:

- ausgehende Anrufe
- eingehende Anrufe
- eingehende Textnachrichten (SMS) oder
- eingehende Multimedia-Nachrichten (MMS)

Um die Regeln nur für einen bestimmten Zeitraum festzulegen, deaktivieren Sie unten die Option **Immer** und wählen Sie die Daten und Uhrzeiten aus, an denen die Regel angewendet werden soll. Standardmäßig sind alle Wochentage ausgewählt. Diese Funktion ist beispielsweise hilfreich, wenn Sie nachts oder am Wochenende nicht gestört werden möchten.

HINWEIS: Wenn Sie im Ausland unterwegs sind, müssen Sie den Rufnummern in der Liste die Landesvorwahl hinzufügen (z. B. +49 711 123).

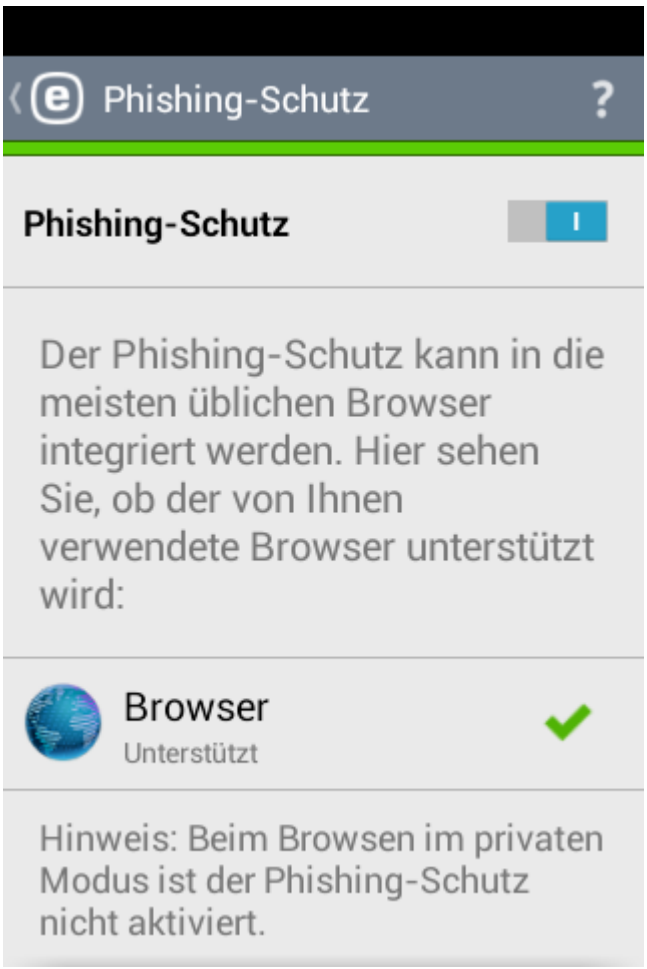
6.2 Verlauf

Im Abschnitt **Verlauf** können Sie die vom SMS- und Anruffilter blockierten und zugelassenen Anrufe und Nachrichten anzeigen. Jeder Log-Eintrag enthält Name, Datum und Uhrzeit des Ereignisses sowie die dazugehörige Telefonnummer. Die Logs zu SMS- und MMS-Nachrichten enthalten außerdem den Nachrichtentext.

Wenn Sie eine mit einer blockierten Telefonnummer oder einem blockierten Kontakt verbundene Regel ändern möchten, wählen Sie den Eintrag durch Antippen aus der Liste aus. Tippen Sie dann auf das Symbol .

Um einen Eintrag aus der Liste zu entfernen, wählen Sie ihn aus und tippen Sie auf das Symbol . Um mehrere Einträge zu entfernen, tippen Sie einen der Einträge an und halten Sie ihn ausgewählt. Wählen Sie dann alle zu entfernenden Einträge aus und tippen Sie auf das Symbol .

7. Phishing-Schutz


Phishing-Schutz
Phishing-Schutz
Der Phishing-Schutz kann in die meisten üblichen Browser integriert werden. Hier sehen Sie, ob der von Ihnen verwendete Browser unterstützt wird:
Browser
Unterstützt
Hinweis: Beim Browsen im privaten Modus ist der Phishing-Schutz nicht aktiviert.

Der Begrif *Phishing* beschreibt kriminelles Handeln, bei dem Social Engineering (die Manipulation von Benutzern zum Erlangen von vertraulichen Informationen) eingesetzt wird. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Informationen wie Bankkontonummern, Kreditkartendaten, PIN-Nummer oder Benutzernamen und Passwörter zu erlangen.

Wir empfehlen, den **Phishing-Schutz** aktiviert zu lassen. Das Modul blockiert alle Phishing-Angriffe von Websites und Domänen, die in der ESET-Malware-Datenbank enthalten sind, und zeigt eine Warnmeldung an, die Sie über den Angriff informiert.

Der Phishing-Schutz kann in die meisten üblichen Webbrowser integriert werden, die für Android erhältlich sind (wie Chrome oder der standardmäßige Android-Webbrowser). Die Liste der unterstützten Browser wurde vor der Veröffentlichung der installierten Version von ESET Mobile Security bestätigt.

Um zu überprüfen, ob der auf Ihrem Gerät installierte Browser von ESET Mobile Security unterstützt wird, tippen Sie auf den Browsernamen. ESET Mobile Security überprüft die Kompatibilität mit dem aktuellen Browser.

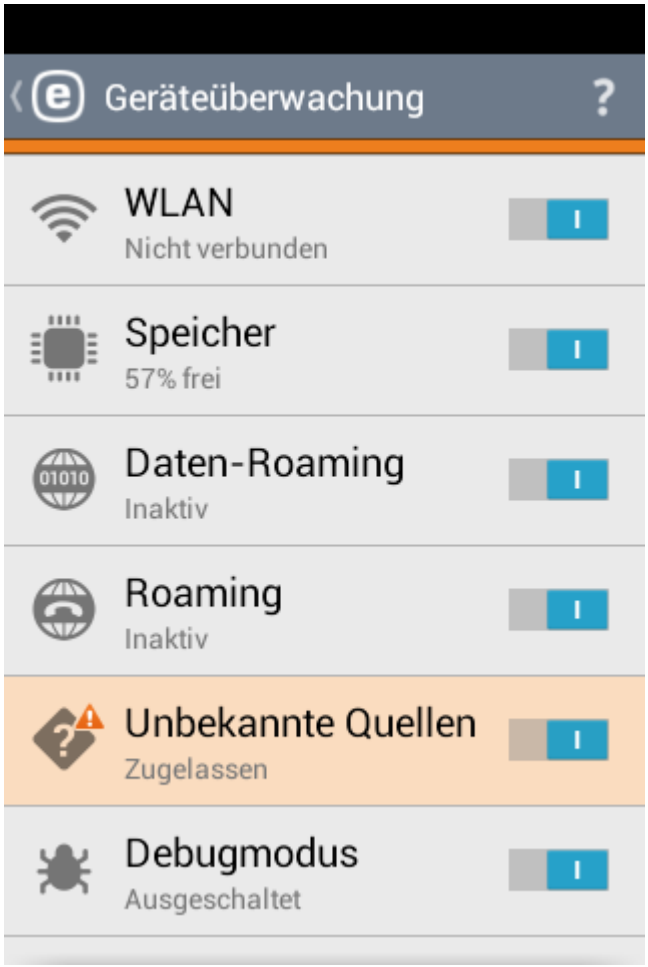
HINWEIS: Der Phishing-Schutz bietet keinen Schutz beim Browsen im Privatmodus.

8. Sicherheits-Audit

Mit dem **Sicherheits-Audit** können Sie wichtige Geräteeinstellungen und Berechtigungen überwachen und ändern, um Sicherheitsrisiken vorzubeugen.

Sie können das Sicherheits-Audit und die entsprechenden Komponenten über folgende Schaltflächen ein- und ausschalten:

8.1 Geräteüberwachung

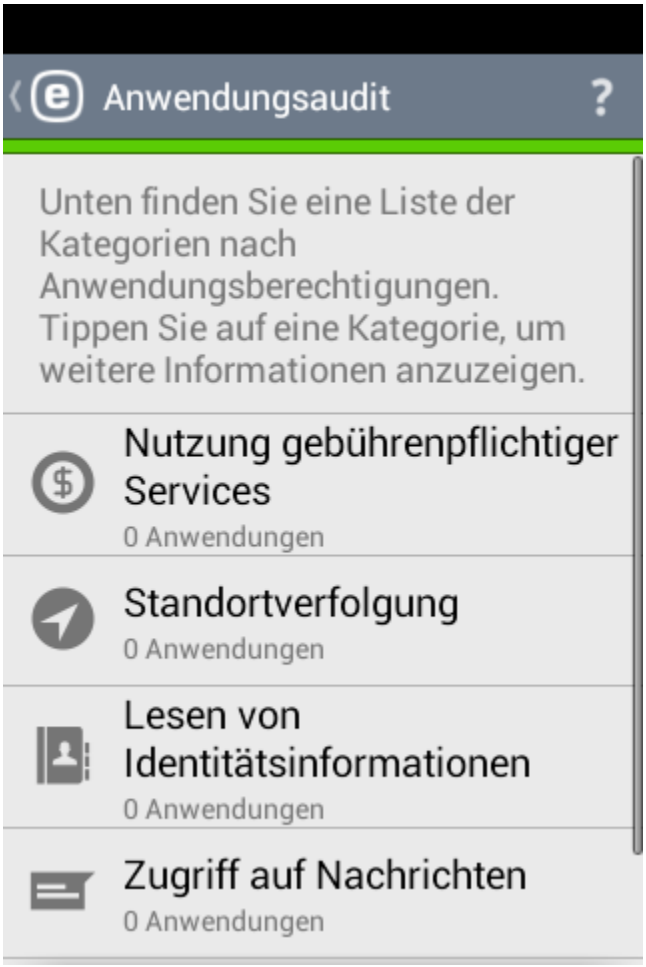


Im Bereich **Geräteüberwachung** können Sie festlegen, welche Gerätekomponenten von ESET Mobile Security überwacht werden.

Tippen auf Sie eine Option, um eine detaillierte Beschreibung und den aktuellen Status der Option anzuzeigen.

Bestimmte Optionen wie **Unbekannte Herkunft** und **Debugmodus** können durch Tippen auf **Einstellungen ändern** geändert werden. Damit wird der Bildschirm mit den Einstellungen des Android-Betriebssystems geöffnet.

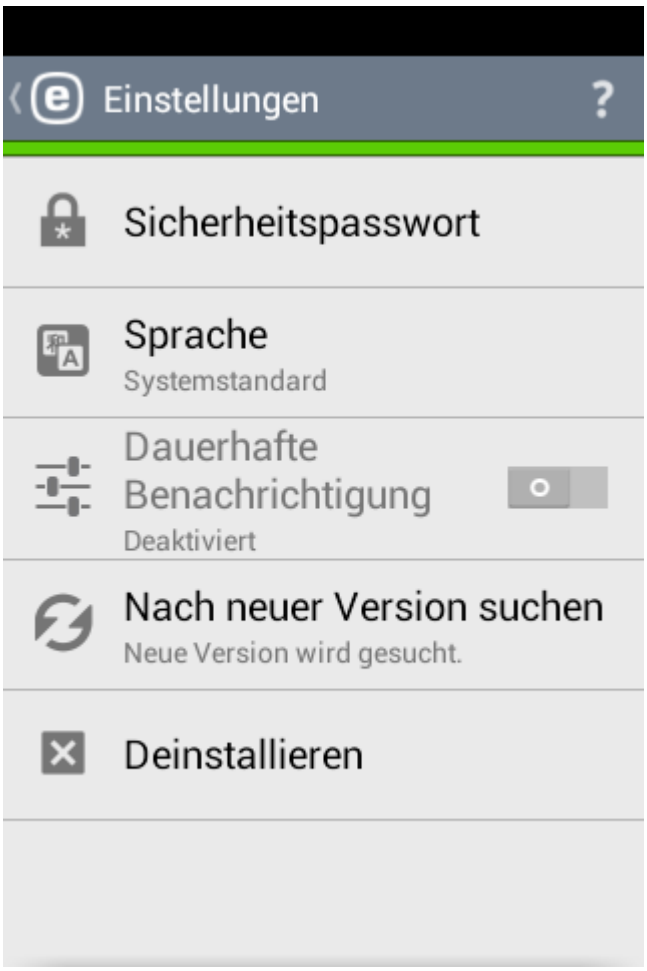
8.2 Anwendungsaudit



Bestimmte auf Ihrem Gerät installierte Anwendungen greifen möglicherweise auf Dienste zu, die gebührenpflichtig sind, Ihren Standort ermitteln oder persönliche Daten, Kontakte oder Textnachrichten lesen. ESET Mobile Security bietet eine Auditfunktion zu diesen Anwendungen.

Im Bereich **Anwendungsaudit** wird eine Liste der nach Kategorien sortierten Anwendungen angezeigt. Tippen Sie auf eine Kategorie, um eine detaillierte Beschreibung anzuzeigen. Tippen Sie auf eine einzelne Anwendung, um Details zu den Berechtigungen der Anwendung anzuzeigen.

9. Einstellungen



Sicherheitspasswort
Unter dieser Option können Sie ein neues Sicherheitspasswort festlegen oder das vorhandene Passwort ändern. Weitere Informationen finden Sie im Abschnitt Sicherheitspasswort 16.

Sprache
Standardmäßig wird ESET Mobile Security in der Sprache installiert, die in den Sprach- und Tastatureinstellungen (Android-Betriebssystem) Ihres Telefons als Systemgebietsschema eingerichtet ist. Um die Anzeigesprache der Benutzeroberfläche zu ändern, tippen Sie auf **Sprache** und wählen Sie die gewünschte Sprache aus.

Dauerhafte Benachrichtigung

Das Meldungssymbol von ESET Mobile Security wird links oben auf dem Bildschirm angezeigt (Android-Statusleiste). Wenn Sie nicht möchten, dass das Symbol angezeigt wird, deaktivieren Sie die **Dauerhafte Benachrichtigung**.

Nach neuer Version suchen
Um einen maximalen Schutz zu gewährleisten, sollten Sie stets die aktuellste Version von ESET Mobile Security nutzen. Tippen Sie auf **Nach neuer Version suchen**, um zu prüfen, ob eine neuere Version zum Download bereitsteht.

Deinstallieren
Um ESET Mobile Security zu deinstallieren, nutzen Sie den Assistenten zum **Deinstallieren**. ESET Mobile Security und die Quarantäneordner werden unwiderruflich gelöscht.

9.1 Sicherheitspasswort

Ihr **Sicherheitspasswort** wird zum Entsperren des Geräts, zum Zugriff auf passwortgeschützte Funktionen (z. B. Anti-Theft) und zur Deinstallation von ESET Mobile Security benötigt. Über die Option **Erinnerung** können Sie einen Hinweis festlegen, der angezeigt wird, falls Sie Ihr Passwort vergessen.

Falls Sie Ihr Passwort einmal vergessen, können Sie eine SMS von einer Nummer aus Ihrer Liste Vertrauenswürdige Freunde 10 an Ihre Mobilfunknummer schicken. Diese SMS muss das folgende Format haben:
eset remote reset
Ihr Passwort wird zurückgesetzt. Anschließend können Sie ein neues Passwort festlegen.

Wenn Sie vor dem Sperren des Geräts keinen vertrauenswürdigen Freund festgelegt hatten, können Sie eine Anfrage zum Zurücksetzen des Passworts senden. Diese Option wird nach 2 erfolglosen Passworteingabeversuchen auf dem Telefon aktiviert. Sie erhalten an der E-Mail-Adresse Ihres Google-Kontos bzw. der unter **Anti-Theft** > **Meine Kontaktdetails** festgelegten Adresse eine E-Mail mit einem Code zum Entsperren des Geräts. Geben Sie diesen Code am Telefon ein. Legen Sie nach dem Entsperren des Geräts unter **Einstellungen** > **Passwort** ein neues Sicherheitspasswort ein.

WICHTIGER HINWEIS: Wählen Sie Passwörter sorgsam aus. Kombinieren Sie Klein- und Großbuchstaben und Zahlen, um die Passwortstärke zu erhöhen und anderen Personen das Erraten Ihres Passworts zu erschweren.

10. Support

Bei allgemeinen oder technischen Fragen zu ESET Mobile Security oder einem anderen Produkt von ESET stehen Ihnen die ESET-Supportmitarbeiter gerne zur Verfügung.

Um direkt vom Gerät aus eine Supportanfrage zu senden, tippen Sie auf das Menüsymbol im Hauptbildschirm von ESET Mobile Security (oder drücken Sie die Taste **MENÜ** am Gerät) und tippen Sie dann auf **Support** > **Support**. Füllen Sie alle erforderlichen Felder aus.

ESET Mobile Security bietet umfangreiche Logging-Funktionen, die bei der Diagnose technischer Probleme helfen. Um ein detailliertes Anwendungs-Log an ESET zu senden, aktivieren Sie **Anwendungs-Log** (standardmäßig aktiviert). Tippen Sie auf **Senden**, um die Anfrage zu senden. Ein ESET-Supportmitarbeiter nimmt unter der angegebenen E-Mail-Adresse Kontakt mit Ihnen auf.